Ricardo A. Vittoni - FSS

Nápoles 3139 - C1431DEA - Cdad. de Buenos Aires - Cel. (11) 15 4416-8977 - ravittoni@gmail.com

SISTEMAS DE SEGURIDAD PARA QUEMADORES (BMS)

SAFETY NOTE SN - 3121

FUNCIONES INSTRUMENTADAS DE SEGURIDAD PARA QUEMADORES DE CALDERAS Y HORNOS

1. Diseño Conceptual de un Sistema de Seguridad para Quemadores (BMS)

A fin de implementar un Sistema de Seguridad para Quemadores (BMS) que permita prevenir la explosión de la Caldera o del Horno de Proceso a proteger, de acuerdo con las Normas prescriptivas NFPA 86, FM 7605, FM 7610 y de performance de seguridad IEC 61508, IEC 61511 e ISA S84, con un Nivel de Integridad SIL 2 (valor de integridad promedio usualmente asignado para este tipo de aplicaciones), deberán tenerse en cuenta las siguientes consideraciones.

En primer lugar, **deberán usarse detectores de llama de alta discriminación** (sobre todo cuando se trate de Calderas u Hornos de múltiples quemadores), para lograr una correcta detección de la llama del quemador sin confusión con otras fuentes de radiación (paredes del hogar, llamas de quemadores vecinos), ya que **la continua salida de gas desde un quemador apagado podrá generar una explosión destructiva**.

Una explosión destructiva constituye el riesgo inherente más alto en este tipo de aplicaciones.
Este riesgo se calcula (en forma simplificada), como **el producto entre la probabilidad de que se produzca una explosión destructiva y la magnitud del daño que pudiera ocasionar dicha explosión** (daño severo o muerte de personas presentes en el área de la explosión, valor del equipamiento destruído, lucro cesante del proceso afectado, etc.), en caso de no implementarse un Sistema de Seguridad BMS.

A fin de reducir el nivel del riesgo de que ocurra dicha explosión **deberá proveerse un Sistema BMS de Alta Integridad que provea Funciones Instrumentadas de Seguridad (SIF) cuyo Nivel SIL sea tal que se garantice que cualquier quemador que se haya apagado sea puesto inmediatamente fuera de servicio** (SIF de shut-off del quemador por apagado de llama).

Estas SIF, independientes por cada Quemador, deberán utilizar Detectores de Llama, secuencias lógicas dentro del Safety Logic Solver del BMS y Válvulas de Shut-off de combustible **también independientes para cada quemador**.

El Nivel de Integridad Segura (SIL) de cada una de esas Funciones de Seguridad (SIF) **dependerá del nivel de riesgo tolerable establecido por el Usuario y del nivel de riesgo inherente de la aplicación**.

El Usuario deberá definir, por lo tanto, el **PFD_{avg}** (Probaility of Failure on Demand promedio) o el **SIL_{avg}** (SIL promedio) de las SIF que deberá proveer el Sistema de Seguridad BMS**, basando esta definición en un Análisis de Riesgo preliminar** (HAZAN, FTA, LOPA, etc.).

Asimismo, el Usuario **deberá definir si el Sistema BMS debe ser solamente FAILSAFE o FAILSAFE / FAULT TOLERANT**.
La diferencia fundamental radica en las pérdidas por lucro cesante tolerables por el Usuario.
Es decir, **un sistema FAILSAFE accionará ante la mínima sospecha de situación de peligro deteniendo el proceso**, incluso cuando se trate de una “falsa alarma” (a esta detención por falsa alarma se la conoce como “falla espuria segura” o “nuisance trip” y su probabilidad de ocurrencia o “PFS” se calcula como cantidad de fallas seguras que se producirán por año).

El lucro cesante se deriva generalmente del hecho que, luego de una parada del proceso, se requieren varias horas (y a veces días) para rearrancar el mismo.
Es decir, una **falla espuria segura** no causará daños al personal, al equipamiento o al medio ambiente, pero **detendrá el proceso causando daños económicos al Usuario**.

Cuando se decida utilizar un Sistema BMS FAILSAFE / FAULT TOLERANT, **la probabilidad de tener paradas espurias y por lo tanto pérdidas económicas será reducida al mínimo** (dependiendo esta reducción del nivel de disponibilidad de todo el Sistema).

Para el Sistema BMS objeto del presente análisis, se asume que **el Usuario ha definido como objetivo un SIL_{avg} de Nivel 2 (SIL_{avg} = 2)**, valor usual en la Industria de Procesos.

Teniendo en cuenta el Ciclo de Vida de la IEC 61508 esto significa que:

a) Por tratarse de un SIL_{avg} = 2 existirán SIF de niveles SIL 1, SIL 2 **y SIL 3**

Varios estudios demuestran que en todo proceso de Nivel SIL 2 (promedio), existe al menos una SIF de Nivel SIL 3. Estadísticas realizadas en varias instalaciones de Sistemas Instrumentados de Seguridad (SIS) alrededor del mundo demuestran que, en promedio**, alrededor de un 15% de las SIF de un Sistema SIS son de Nivel SIL 3** ("Future trends in SIS Logic Solvers", Eng. Kirk Fontenot).

Además de las "SIF de shut-off por apagado de llama", las cuales constituyen el último nivel de protección contra la explosión y poseen generalmente **Nivel SIL 2 / SIL 3**), el Sistema BMS deberá proveer SIF de niveles SIL 1 y SIL 2 preventivas, como lo son las "SIF de shut-off" por alta o baja presión de gas, por baja presión o falta de aire de combustión, etc..

Cabe aclarar que el Nivel SIL define un rango de protección que va desde un valor mínimo a un valor máximo de Probabilidad de Falla en Demanda (PFD).
Para el Nivel SIL 2 la PFD debe ser menor que 1E-2 y mayor que 1E-3, mientras que para SIL 3 la PFD oscila entre 1E-3 y 1E-4. El decir Nivel SIL 2 / SIL 3 significa que estas SIF requieren Niveles de PFD cuyo valor está en el orden de 1E-3.

b) Las SIF de Nivel SIL 2 / SIL 3 podrán ser reducidas a SIL 2 utilizando capas adicionales de protección y/o **deberán utilizarse arquitecturas de protección SIL 3** para ejecutar dichas SIF.

c) El Nivel de Protección SIL_{avg} = 2 deberá ser mantenido a lo largo de todo el Ciclo de Vida por medio de la prueba periódica, a intervalos regulares, del funcionamiento de todas las SIF

Nápoles 3139 - C1431DEA - Cdad. de Buenos Aires - Cel. (11) 15 4416-8977 - ravittoni@gmail.com

1.1 SIF de shut-off de quemadores por apagado de llama

1.1.1 Sistemas de Monitoreo de Llama

El primer eslabón en la cadena de seguridad de la "SIF de Shut-off por apagado de llama" lo constituyen los Sistemas de Monitoreo de Llama.
Como se dijo anteriormente, los Sistemas de Monitoreo de llama **deberán utilizar detectores FAILSAFE de alta discriminación**, para lograr una correcta detección de la llama del quemador sin confusión con otras fuentes de radiación.

Como se explicara también anteriormente, se considera que estas SIF son de Nivel SIL 2 / SIL 3. Para garantizar este Nivel SIL con detectores de llama standard se necesitara utilizar tres detectores en votación 2oo3 por cada Quemador.
Sin embargo, la utilización de **Sistemas de Monitoreo de Llama FAILSAFE con Alta Cobertura de Diagnóstico hará que sólo se necesiten dos detectores en votación 1oo2** para garantizar un Nivel SIL2 / SIL3.

Estos Sistemas de Monitoreo deberán **estar aprobados por Organismos Independientes de Certificación (FM, TÜV, CSA, etc.) como sistemas de protección de quemadores** según la Norma FM 7610 "Combustion Safeguards and Flame Sensing Systems" y, muy probablemente, deberán poseer **certificación para su utilización en áreas clasificadas** Class I, Div 2, Groups B, C, y D (Zone 2), en caso que se defina el área donde irá instalado el cabezal de detección como Área Clasificada según NFPA 70 Art. 500 (ó IEC 60079).

1.1.2 Programmable Electronic Logic Controller (PESC)

El segundo eslabón en la cadena de seguridad de las "SIF de shut-off por apagado de llama" y el corazón del Sistema BMS, responsable además de la ejecución de todas las SIF, es el Safety Logic Solver o **Programmable Electronic Safety-related Controller** (PESC), como lo define la Norma IEC 61508.

El PESC se encargará de ejecutar las secuencias lógicas de encendido y apagado seguro de todos los quemadores. Estas secuencias lógicas estarán compuestas por la ejecución combinada de varias SIF, de distinto Nivel SIL, entre ellas, las SIF de shutt-off por apagado de llama.

En el caso de los Sistemas BMS, el PESC deberá ser del tipo FAILSAFE De-Energize-To-Trip y estar homologado según la Norma IEC 61508 tal como establece la Norma FM 7605, "Programmable Logic Control Based Burner Management Systems" (en los casos en los que se requiera además de Alta Disponibilidad Operativa con un muy bajo nivel de PFS, como se dijo en el punto 1, el PESC deberá ser FAILSAFE / FAULT TOLERANT).

La Norma IEC 61508 es muy específica con respecto a la utilización de equipamiento Eléctrico, Electrónico o Electrónico Programable en aplicaciones de seguridad: **la ejecución de Funciones de Seguridad (SIF) será responsabilidad de un Logic Solver Certificado por un Organismo Independiente, con un Nivel de Integridad (SIL) adecuado para el Nivel de Riesgo de cada SIF que deba ejecutar**.

No podrá utilizarse, por lo tanto, **ninguno de los controladores de secuencia de encendido de quemadores y supervisión de llama** utilizados antiguamente para este tipo de aplicaciones**, a menos que posean esta Certificación de Nivel de Integridad**.

Es decir, **las SIF que ejecutará el PESC deberán garantizar el Nivel SIL en todas sus partes de hardware** (CPU y módulos del PESC, dispositivos de campo), **en su instalación** (conexiones a dispositivos de campo debidamente implementadas) **y en su software de aplicación**, observando estrictamente las Normas Prescriptivas NFPA 86 y FM 7605 como así también las Normas de Performance IEC 61508, IEC 61511 e ISA S84.

Como también se explicó en el punto 1, el Nivel SIL de las SIF que ejecutará el PESC dependerá fundamentalmente del Nivel SIL_{avg} definido por el Usuario.
Como la existencia de una única SIF de Nivel SIL 3 requerirá de un PESC apto para ese Nivel de Integridad, **el PESC de un Sistema BMS deberá estar certificado para la ejecución de SIF de Nivel SIL 3** ("Future trends in SIS Logic Solvers", Eng. Kirk Fontenot).

El PESC del Sistema BMS deberá incluir el suministro de **un terminal de texto independiente de cualquier otro sistema de visualización,** que mostrará todos los **mensajes de advertencia y alarma** relacionados con cada situación anormal en la cual intervenga el Sistema de Seguridad.

1.1.3 Válvulas de Bloqueos y Venteos de Gas

El último eslabón en la cadena de seguridad de las "SIF de shut-off por apagado de llama" y quizá el más importante desde el punto de vista que es éste el que efectivamente realiza el corte de suministro del combustible y pertenece, por tanto, a ésta y otras SIF del Sistema BMS, lo constituyen las Válvulas de Shut-off y Venteo.

Estas **Válvulas deben estar aprobadas por FM** u organismos similares **"para su uso específico como válvulas de shut-off de quemadores" según FM 7400, "Liquid and Gas Safety Shutoff Valves", para el uso específico de Shut-off Seguro de quemadores, con cierre hermético superior a Class VI según ANSI/FCI 70-2.**

El corte de combustible según NFPA **debe realizarse utilizando dos válvulas de Shutt-off en cascada, con una válvula de Venteo conectada en el tramo que las une, para la alimentación de cada quemador**.

Para aplicaciones de Nivel SIL 2 / SIL 3, además, **los cierres shut-off deben ser de nivel de hermeticidad garantizado, leakage Class VI según ANSI/FCI 70-2**, de larga vida útil, dado el bajo nivel de prueba manual en este tipo de instalaciones (generalmente no menos de una vez cada 12 meses), para sostener la garantía de integridad según los pasos del Safety Life Cycle indicado por las IEC 61508.

Es imprescindible, además, que el accionamiento de las Válvulas de Bloqueo sea FAILSAFE (FAIL CLOSED), es decir, que ante cualquier falla las Válvulas de Bloqueo cierren el paso de gas y que **las Válvulas de Venteo sean FAILSAFE (FAIL OPEN)**, es decir, que ante cualquier falla el venteo se abra.

No obstante, deberán tomarse precauciones a fin de evitar que un Venteo se abra cuando alguno de los dos Bloqueos esté abierto, para lo cual **es necesario monitorear el estado (apertura y cierre) de cada Válvula**.

Esto hace que sea necesaria la implementación de SIF con lógica de enclavamiento en el PESC, con el consecuente cableado de señales de entrada y salida para cada válvula (tres solenoides y seis detectores de posición por cada quemador).

Como configuración alternativa a este conjunto (dos válvulas de shut-off y una de venteo), se podrán utilizar "válvulas de triple efecto".

Estas válvulas **tienen un único cuerpo y ejecutan, sobre un único vástago, y sin errores o desfasajes**, las tres acciones mencionadas, dos de Shut-off y una de Venteo, **utilizando la tercera parte de las señales necesarias para una solución convencional y sin necesidad de la SIF de enclavamiento en el PESC**.
De esta forma, **la instalación ocupará muy poco espacio y tendrá un costo de instalación mucho más bajo** (por requerir la tercera parte de bridas, tramos de cañerías, soldaduras, cañerías y cableados eléctricos, mano de obra, etc., que se necesita para una instalación convencional de tres válvulas por cada alimentación).
Se disminuirán además las tareas de mantenimiento preventivo y correctivo.

Se preferirá la utilización de solenoides de comando neúmatico con bobinas de 24 Vdc, de conexión directa al PESC, para evitar la utilización de relés de aislación y su correspondiente lógica con integridad SIL 2 / SIL 3.

1.2 Otras SIF de prevención de explosiones

Elementos fundamentales para la ejecución de las SIF de prevención del Sistema BMS (con niveles de integridad SIL 1 y/o SIL 2), son los Presostatos de gas combustible, los Transmisores de Presión del aire de combustión, y los Sensores de Posición de Válvulas y Dampers.

A fin de garantizar el Nivel SIL de cada SIF **deberán utilizarse dispositivos de contactos supervisados o transmisores analógicos, debiéndose implementar las votaciones necesarias que garanticen el PFD correspondiente**.

Cuando se utilicen Presostatos (dispositivos de contacto), **la obtención del Nivel SIL 2 se garantizará con la implementación de dos detectores en votación 1oo2**. Asimismo, **los contactos de cada uno de ellos deberán estar supervisados para detectar eventuales corto-circuitos y/o cables a masa y/o cables cortados**.

Cuando se utilicen Transmisores de Presión, se dará preferencia a los que posean Cobertura de Diagnóstico superior al 65% y **en lo posible que sean certificados para aplicaciones de Nivel SIL 2** (en este caso un solo transmisor será suficiente para garantizar este Nivel de Integridad).

Para la detección de posición de válvulas y dampers, **deberán utilizarse configuraciones de contactos en votación cuando se utilicen microswitches estándar**.
En caso de utilizar detectores de posición **certificados para Categoría 4 según EN 954, un solo detector garantizará un Nivel de Integridad SIL 2** (o SIL 3).

2. Ingeniería del Sistema BMS

Tal como establece la IEC 61508 para el Ciclo de Vida del Sistema de Seguridad, **la Ingeniería del Sistema en su totalidad**, incluyendo las correspondientes a la instalación de los elementos de campo y a la instalación, programación y puesta en marcha del PESC, **deberá ejecutarse de forma tal de garantizar el Nivel de Integridad SIL_{avg} y el Nivel SIL** (SIL 1, 2 ó 3) **de cada función SIF**.

2.1 Ingeniería de la Instrumentación

Seguramente resultará conveniente o necesario ejecutar “a priori” un HAZOP del Proceso previsto, para verificar el Nivel de Integridad SIL (promedio) especificado y definir las cantidades y tipos definitivos de los componentes de campo a utilizar.

Las exigencias actuales de seguridad obligan a un trabajo de Ingeniería de Instrumentación que diseñe cuidadosamente un eficiente esquema de operatividad y sus automatismos de protección de acuerdo con las Normas.

Esta Ingeniería **deberá ser desarrollada por un Integrador de Sistemas de Seguridad con alto grado de experiencia y confiabilidad**, incluyendo la provisión de típicos de montaje y un listado completo de la instrumentación necesaria para cumplir con el Nivel SIL y con la disponibilidad del Sistema requeridos por el Usuario.

2.2 Ingeniería de Programación, Commissioning y Puesta en Marcha del PESC

Por tratarse de un Sistema de Seguridad homologado con las Normas IEC 61508, IEC 61511 e ISA S84.01, **la programación del PESC debe seguir estrictos criterios de programación, validación y verificación de las secuencias y algoritmos lógicos correspondientes a cada SIF**, sobre todo para aquéllas de Nivel SIL 2 / SIL 3 relacionadas con el shut-off por apagado de quemadores.

Para la programación de SIF de Niveles SIL 2 / SIL 3 se utilizarán preferentemente **Bloques de Programación Certificados y Programación Estructurada.**
Se proveerá además un diagrama de flujo para cada SIF, **indicando claramente las previsiones de seguridad tomadas para cada condición de falla**.

Se proveerá además **un listado completo de mensajes de advertencia y alarma** (los cuales serán **mostrados en un terminal de texto independiente de cualquier otro sistema de visualización** provisto junto con el PESC), para cada situación en la cual intervenga el Sistema de Seguridad.

Asimismo, la provisión del FAT (Factory Accepttance Test), con simulación operativa de todas las SIF y los servicios de OSAT (On-Site Acceptance Test), Commissioning y Puesta en Marcha en Planta del Contratista y/o del Usuario, **deberá estar garantizada por el Integrador del Sistema de Seguridad**.

Ricardo A. Vittoni - FSS
Functional Safety Specialist